PRIVACY ASSOCIATES INTERNATIONAL LLC

Close Encounters of the Third (Party Supplier) Kind

IAPP KnowledgeNet Detroit

May 7, 2015

Agenda

- Intros, announcements and administration
- Discuss privacy aspects of vendor management process
- Time permitting open discussion:

Intro Matters

- New KnowledgeNet Chairs
  - Art, Doris, Keith
- Meeting dates
  - May 7, July 29, September 16, November 5
- Upcoming IAPP Academy
  - Las Vegas September 29 – October 1
- Today's program

Purpose

- Provide a forum to discuss privacy aspects of Vendor management
- Discuss factors to consider with vendor relationships pertaining to
  - Vetting, contracting, monitoring and resolving disputes
- Engage in an interactive session to highlight concerns and possible solutions from the session learning.

Background

- Organizations are accountable for the protection and appropriate handling of personal data entrusted to them.
- Data protection laws hold organizations accountable for protecting the privacy of any personal data accessed by their data processors or third-party vendors.
- Organizations spend resources to screen vendors primarily to:
  - 1) avoid potential legal liability if the vendor for any reason fails to keep necessary information private; and
  - (2) avoid of loss of goodwill with customers, employees, and others whose personal information has been entrusted to the organization.

Background

- Organizations know the personal data protection requirements and obligations they are required to follow.
- Organizations want to maintain a comparable level of personal data protection and security from third party vendors.
- Organizations must determine what they will require in data protection requirements applicable to the selection of prospective vendors, as well as requirements those vendors are expected to follow.

PAI

Background

- A matrix of requirements applicable to the type(s) of personal data involved will help define necessary protections.
- The level of information about a vendor may vary by sensitivity and volume of personal data involved and any special requirements associated with the type of data.
- Important to determine and specify the vendor characteristics and your performance requirements to ensure you engage vendors capable of processing and safeguarding the personal data you entrust to them as they work for your organization or on its behalf.

VETTING

Determining Attributes

In determining attributes desired in a vendor, and the standards that could be included in the contractual relationship, consider:

- Reputation/Standing in the Community
- Geographic location
- Industry Specific Experience
- Vendor Actual Operations
- Audits/Business Reviews

Attributes – Reputation

- Are there recent news stories about the vendor?
- What is available through Google or other web searches?
- Is there a reporting service with information about the vendor (e.g. Dunn & Bradstreet type reports, BBB etc.)?
- How long has the vendor been in business?
- Is there litigation in which the vendor is the defendant?
- If there is litigation, are there cases other than minor, normal business matters?
- Is the vendor publicly traded? If so, do the vendor's government document filings provide additional information?
- Would a failure of the vendor's business affect the organization?
- Has the vendor had data breaches in the past? What were the circumstances? Have any deficiencies been addressed?

PAI

Attributes - Geographic location

- Where is the vendor located?
- Do laws, regulations, trade codes or existing contracts to which your organization is subject affect location?
- Does the vendor have an established location?
- Is it owned or leased?
- How long has the vendor conduct business at the location?
- Are there other locations where the vendor does business?

Attributes – Industry Specific Experience

- Does the vendor have experience in your industry?
- How is the vendor regarded by other industry participants?
- Does the vendor have necessary or appropriate certifications regarding their service?
- Is the vendor certified as compliant to a specific or industry specific standard (e.g. ISO, CPI-DSS, NIST etc.)?
- Has the vendor delivered similar services for others and is there a contact or other method to confirm?

Attributes - Vendor Operations

- Does the vendor have documented processes and procedures for processing personal data?
- Has the vendor been subject to any regulatory enforcement or litigation?
- Does the vendor have a documented and operational employee training program?
- Are vendor employees required to sign non-disclosure agreements or confidentiality agreements?
- Are there any special industry-imposed requirements and have they been met?
- Will the vendor need to certify compliance with applicable industry regulations or other similar requirements?

PAI

Attributes - Vendor Operations

- If the industry or business sector your organization participates requires a written contractual undertaking or determination of a particular status (e.g. HIPAA BA, GLBA Supplier) will the vendor or agree to execute the necessary agreement?
- Is the vendor a member or participant in professional or trade associates that require maintenance and adherence to specified standards? (e.g. DMA, NAB, BBB, etc.)
- Will any aspect of the vendor's services be subject to subcontracting?
- If the vendor uses subcontractors, where are the sub-contractors located? If the subcontractors are in other countries, what is the anticipated reaction of your organization's customers? Will there be any adverse consequences from a business standpoint to your organization?

Attributes - Vendor Operations

- Will the vendor use cloud services in its delivery of services?
- If so, what form of cloud services are used (private cloud, public cloud or some other form)?
- How is the information in the cloud protected?
- Will your organization's personal data be comingled with the personal data of other clients of the vendor?
- What type of data segregation will the vendor use? Logic, separate devices, other methods?
- Will vendor's IT personnel be segregated by vendor client or will the employees have access to personal data from multiple clients?

PAI

Attributes - Vendor Operations

- Does the vendor have a written data security plan?
- Does vendor have a physical security plan?
- Does the vendor have a written administrative security plan?
- Does the vendor have a written business continuity plan?
  - Has the plan been used?
  - If so, when was the last time?
  - When was the last time the plan was tested through a table top or similar exercise?

Attributes - Audits/Business Reviews

- When was the vendor's last SOC II audit?
- Does the vendor have a SOC II audit sufficient to address the services it will provide for your organization?
- Will they provide a copy of the audit or arrange an audit to address your concerns?
- Does the audit address the obligations or personal data processing your organization will contract to have them deliver?
- Annual or regular recertification?

Attributes – Use of Tools

- Supplier Information Gathering Questionnaire (SIG) Supplier Information
  - Comes in multiple version e.g. SIG Lite
  - Standardized and computerized
  - SIG Lite addresses 13 categories with 68 questions
- SIG information online
- Nymity Privacy Management Accountability Tool
- Others

Attributes – Use of Tools

- Supplier Information Gathering Questionnaire (SIG) Supplier Information
  - Comes in multiple version e.g. SIG Lite
  - Standardized and computerized
  - SIG Lite addresses 13 categories with 68 questions
- SIG information online
- Nymity Privacy Management Accountability Tool
- Others

CONTRACTING

Contracting

- Create and maintain contract templates that address data privacy obligations so they are consistent across similar vendors
  - different contract templates may be created for different classes of vendors and different types of personal data (e.g. sensitive, non-sensitive) and
  - address data protection legal requirements

Contracting Topics

- Data protection responsibilities
  - acceptable use of personal data
  - use of subcontractors
  - restrictions on further transfers, disclosures or uses,
- Data security requirements,
- Data disposal at contract-end, and
- Breach response obligations

Considerations in Template Contracts Creation and Content

- Access, review, correction and choice
- Audit
- Business continuity
- Compliance with law
- Definitions
- Incident processing and breach response
- Indemnification
- International transfers of personal data to processing vendors

Considerations in Template Contracts Creation and Content

- International transfers of personal data to processing vendors
- Post termination
- Damages
- Security
- Service specification
- Term and Termination
- Use limits
- Vendor employees
- Vendor sub-contracting

Executing Contracts

- Maintain procedures to execute contracts with all vendors processing personal information in the custody of the organization
- Includes:
  - identification of vendor contracts which require specific privacy provisions,
  - alternatives for structuring the legal relationships involved so privity exists between all controllers and processors, and
  - considerations related to authority to execute such agreements.

Executing Contracts

- Entering into appropriate contracts with vendors provides the organization with a means to
  - specify how the information should be treated by the vendor and
  - to transfer financial (but not necessarily reputational) risk for non-performance with the standards to the vendor.
- Appropriate contracts with vendors are also required to avoid fines and lawsuits based on failure to have statutorily required agreements with vendors in place.

Executing Contracts

- Contracts involving the processing of personal information should require incorporation of specific privacy provisions prior to execution
- The structure of contracts with vendors having access to personal information will affect execution procedures
- Privacy requirements can either be:
  - Included in the commercial agreement with the vendor; or
  - Included in a self-standing umbrella privacy agreement with the vendor

Executing Contracts

- It is critical that privity of contract exists between and among each vendor entity accessing personal information and each organizational entity providing personal information
- Individuals signing the vendor agreement or power of attorney must have appropriate internal organizational authority within the entity to do so.
- Create and maintain a record of all executed agreements including personal data

Monitoring

Monitoring Logistics

- Establish thresholds parameters
- Determine:
  - if performed centrally or by business units
  - if key risk factors exist
  - the timing and frequency
  - scope and level

Monitoring

- For performance, measure
  - Financial
  - Compliance
  - Quality
  - Impact on customer satisfaction
  - News events, filings, etc.
- Determine type of audit review:
  - Desk top
  - In person
  - Third party reports, certifications standards

Resolving Disputes

Disputes

- Determine if the vendor is actually in a non-compliant situation and the related facts
- Understand the alternative possible courses of action and their consequences from both a business and legal standpoint
- Have the appropriate individual or group within the organization make a decision as to what action to take after having received input from affected areas in the organization and advice from legal counsel

Resolving Disputes

- Where a vendor has breached its data protection or security requirements under the vendor contract or processing agreement, have procedures to address the non-compliance.
- May include:
  - notifying the vendor of the failure and giving it time to address the non-compliance,
  - aiding the vendor in remediating the failure,
  - terminating the vendor's access to personal data, or
  - in serious cases, terminating the contract entirely